

### **Remarks**

Reconsideration is requested in view of the preceding amendments and the following remarks. Claims 8 and 17 are canceled without prejudice, claims 6, 9-10, 16, 18 and 22 are amended, and new claims 23-29 are submitted for consideration. Upon entry of this Amendment, claims 6-7, 9-11, 16, 18, and 22-29 are in the application.

Support for new claims 23-29 can be found in, for example, the claims as filed.

### **Rejections under 35 U.S.C. § 112**

Claim 22 is rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. This rejection is traversed. According to the Office action, the specification and drawings contain no discussion or illustration of the claimed third processing unit and fourth processing unit. This is incorrect. Fig. 1 shows three processing units 132, 133, 134 and indicates that additional processing units can be provided (note the ellipses extending downward and to the right of the processing element 134). The processing units 132, 133, 134 receive bits  $a_0$ ,  $a_1$ ,  $a_2$ , respectively. Fig. 2 illustrates seven processing units 231-237 that receive bits  $a_0$ ,  $a_1$ ,  $a_2$ ,  $a_3$ ,  $a_4$ ,  $a_5$ ,  $a_6$ , respectively. Figs. 1-2 are discussed in the specification at pages 14-15. In view of the discussion and illustration of multiple processing units in the specification and drawings, withdrawal of this rejection is requested.

### **Rejections under 35 U.S.C. § 102**

Claims 6-11 and 16-18 stand rejected as allegedly anticipated by Guy, U.S. Patent 6,035,317 (hereinafter "Guy"). This rejection is traversed. The rejection of claims 8 and 17 is moot in view of the cancellation of these claims without prejudice.

Amended independent claim 6 recites, in part,

a field-type input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with  $GF(p)$  or  $GF(2^m)$  arithmetic, wherein  $GF(p)$  is a prime field,  $GF(2^m)$  is a binary extension field,  $p$  is a positive prime number, and  $m$  is a positive integer.

Guy does not teach or suggest such a field-type input. The Office action cites Guy, col. 1, lines 7-22, as teaching this feature. This is incorrect. According to Guy,

The invention relates to a modular arithmetic coprocessor comprising two multiplication circuits working in parallel. More specifically, the invention relates to the improvement of a known arithmetic coprocessor enabling the performance of modular operations according to the Montgomery method in order to extend the applications of this coprocessor. The Montgomery method performs modular computations in *a finite field denoted  $GF(2^n)$*  without the performance of divisions. Guy, col. 1, lines 7-16 (emphasis added).

Conventionally, *modular operations on  $GF(2^n)$*  are used in cryptography for applications such as authentication of messages, identification of a user and exchange of keys. Such exemplary applications are described for example in French patent application published under No. 2 679 054. Guy, col. 1, lines 18-22 (emphasis added).

This portion of Guy teaches only  $GF(2^n)$  arithmetic and is silent concerning arithmetic in  $GF(p)$ .

Because Guy does not teach or suggest arithmetic in both  $GF(2^n)$  and  $GF(p)$ , Guy necessarily lacks the recited field-type input that selects between  $GF(2^n)$  and  $GF(p)$  arithmetic, and claim 6 is properly allowable. Dependent claims 7, 9-11, and 22-27 depend from allowable claim 6, and are properly allowable for at least this reason.

Claims 7, 9-11, and 22-27 recite additional features and combinations of features that are not taught or suggested by Guy. For example, claim 9 further recites that “the arithmetic operation selectable with the field-type input is field addition.” As noted above, Guy does not teach arithmetic in  $GF(p)$  and hence necessarily lacks a field-type input that selects between

GF( $2^n$ ) arithmetic and GF(p) arithmetic. The Office action cites Guy as teaching this feature at col. 6, lines 8-17 and col. 6, lines 46-53. This is incorrect. According to these cited portions of Guy,

[A] first addition circuit . . . performs operations of addition between a piece of data stored in the second register and a piece of data produced by the first multiplication circuit, [and]

a second addition circuit . . . performs an operation of addition between a piece of data produced by the first addition circuit and a piece of data given to the second addition circuit by the second multiplication circuit. Guy, col. 6, lines 8-17.

According to one embodiment, the device furthermore comprises a third addition circuit, series-connected with the first addition circuit, that performs addition operations between pieces of data stored in the second and fifth registers and a piece of data produced by the first multiplication circuit and multiplexing means that selectively supplies, to an input of the third addition circuit, the contents of the fifth register or a permanent logic state. Guy, col. 6, lines 46-53.

The cited portions of Guy merely disclose addition circuits, and do not teach or suggest any circuits configured to selected between GF( $2^n$ ) and GF(p) arithmetic as recited in claim 9.

Claim 10 further recites “a dual-field adder in communication with the field-type input.”

As noted above, Guy does not teach or suggest selecting between arithmetic in GF( $2^n$ ) and GF(p) and hence necessarily lacks a dual-field adder and a field-type input. The Office action cites Guy at col. 6, lines 8-17 and 46-53 as teaching such a dual-field adder. The cited portions of Guy are provided above, and merely disclose conventional addition circuits lacking any selection of field type arithmetic. For at least this reason, claim 10 is properly allowable over Guy.

New claim 24 further recites a dual-field adder configured to selectively execute addition corresponding to addition with carry or without carry based on the field-type input. As noted above, Guy does not teach or suggest such a dual-field adder, nor does Guy teach or suggest selecting between addition with carry or without carry. For at least this reason, claim 24 is properly allowable over Guy.

In view of the allowability of claims 7, 9-10, and 22-27 as dependent on allowable independent claim 6, additional reasons for the allowability of these claims are not belabored herein.

Amended independent claim 16 recites a method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising, in part:

processing a first bit of the first parameter with each word of the modulus and each word of the second parameter to produce a first series of intermediate values and a contribution to the Montgomery product based on the first bit;  
processing a second bit of the first parameter with each word of the modulus and each word of the second parameter, and a corresponding intermediate value from the first series of intermediate values to produce a second series of intermediate values and a contribution to the Montgomery product based on the second bit, *wherein the first series of intermediate values and the second series of intermediate values are determined based on a field-type input that selects an arithmetic operation to be performed in accordance with  $GF(p)$  or  $GF(2^m)$  arithmetic, wherein  $GF(p)$  is a prime field,  $GF(2^m)$  is a binary extension field,  $p$  is a positive prime number, and  $m$  is a positive integer.* (emphasis added)

The Office action cites Guy at col. 6, lines 8-17 and col. 6, lines 46-53 as teaching a field-type input associated with selection of an addition operation corresponding to addition with or without carry. This is incorrect. These cited portions of Guy are provided above, and are silent concerning a field-type input of any kind, or selection of an arithmetic operation. For at least this reason, claim 16 and dependent claims 18 and 28-29 are properly allowable over Guy.

Dependent claims 18 and 28-29 recite additional features and combinations of features that are not found in Guy and are allowable for additional reasons as well. In view of the allowability of dependent claims 18 and 28-29 as dependent on allowable claim 16, additional reasons for the allowability of these claims are not belabored further.

### Rejections under 35 U.S.C. § 103

Claim 22 stands rejected as allegedly obvious in view of Guy. This rejection is traversed.

Claim 22 depends from allowable claim 6 and is properly allowable for at least this reason.

### Conclusion

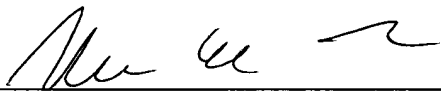
If view of the preceding, all claims are believed to be in condition for allowance and action to such end is requested. If a telephone conference would expedite prosecution, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

One World Trade Center, Suite 1600  
121 S.W. Salmon Street  
Portland, Oregon 97204  
Telephone: (503) 595-5300  
Facsimile: (503) 595-5301

By

  
\_\_\_\_\_  
Michael D. Jones  
Registration No. 41,879